

CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2



NEW QUESTION 1

Which of the following file extensions are commonly used to install applications on a macOS machine? (Select THREE).

- A. .mac
- B. .Pkg
- C. .deb
- D. .dmg
- E. .msi
- F. .appx
- G. .app
- H. .apk

Answer: BDG

Explanation:

<https://support.microsoft.com/en-us/windows/common-file-name-extensions-in-windows-da4a4430-8e76-89c5>

.pkg and .dmg are files used to distribute and install applications on macOS. .pkg files are installer packages that may contain multiple files and executable code, while .dmg files are disk images that can contain a single bundled application or multiple applications. .app files are typically the main executable files for macOS applications. The other options listed are file extensions for applications or installers on other platforms (such as .deb for Debian-based Linux systems, .msi for Windows, and .apk for Android). This information is covered in the CompTia A+ Core2 documents/guide under the Mac OS section.

NEW QUESTION 2

Upon downloading a new ISO, an administrator is presented with the following string: 59d15a16ce90cBcc97fa7c211b767aB

Which of the following BEST describes the purpose of this string?

- A. XSS verification
- B. AES-256 verification
- C. Hash verification
- D. Digital signature verification

Answer: C

Explanation:

Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source¹

NEW QUESTION 3

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickers to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.

TEST QUESTION

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

INSTRUCTIONS
Click on individual tickets to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Show QuestionReset All Answers

Details

	Date	Priority	
ling to boot. Screen l...	7/13/2022	High	
o access Z: on my co...	7/13/2022	Low	

No Ticket Selected

Please select a ticket from the list

Details			
<div> <div>ing to boot. Screen i...</div> <div>g</div> </div>	Date	Priority	
	7/13/2022	High	
<div> <div>to access Z: on my co...</div> <div>0</div> </div>	7/13/2022	Low	
Subject		PC is failing to boot. Screen is displaying error message, see attachment	
Attachments		bootmgr not found.png	
Issue		<div></div>	
Resolution		<div></div>	
Verify/Resolve		<div></div>	

The screenshot shows the Windows Troubleshooting Center interface. On the left, a list of issues is displayed with columns for Date and Priority. One issue is highlighted with a red 'High' priority button. The main pane shows details for a selected issue: #6675309, Open, High priority, Category: Technical / Bug Reports, Assigned To: helpdesk@fictional.com, Assigned Date: 7/13/2022. The Subject is 'PC is failing to boot. Screen is displaying error message, see attachment.' and the Attachments include a link to 'bootmgr not found.png'. Below the details, there is a dropdown menu for 'Issue' and a 'Resolution' section with a list of steps. The 'Verify/Resolve' section is also visible, showing a list of commands to run in the command prompt.

Details

#6675309 Open
 Priority High
 Category Technical / Bug Reports
 Assigned To helpdesk@fictional.com
 Assigned Date 7/13/2022

Subject PC is failing to boot. Screen is displaying error message, see attachment.

Attachments [bootmgr not found.png](#)

Issue

Resolution

- Corrupt OS
- Recent Windows Updates
- Graphics Drive Updates
- BSOD
- Printing Issues
- Limited Network Connectivity
- Services Failed to Start
- User Profile is Corrupted
- Application Crash
- User cannot access shared resource
- URL contains typo
- Reinstall Operating System
- Rollback Updates
- Rollback Drivers
- Repair Application
- Restart Print Spooler
- Disable Network Adapter
- Update Network Drivers
- Refresh DHCP
- Rebuild Windows Profile
- Apply Updates
- Repair Installation
- Restore from Recovery Partition
- Remap network drive
- Verify integrity of disk drive
- Initiate screen share session with user
- Windows recovery environment
- Inform user of AUP violation

Verify/Resolve

- chkdsk
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- bootrec

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Details

#8675309

Open

Priority

High

Category

Technical / Bug Reports

Assigned To

helpdesk@fictional.com

Assigned Date

7/13/2022

Subject

PC is failing to boot. Screen is displaying error message, see attachment

Attachments

[bootmgr not found.png](#)

Issue

Corrupt OS

Resolution

Reinstall Operating System

Verify/Resolve

chkdsk

Close Ticket

NEW QUESTION 4

A technician is reimaging a desktop PC. The technician connects the PC to the network and powers it on. The technician attempts to boot the computer via the NIC to image the computer, but this method does not work. Which of the following is the MOST likely reason the computer is unable to boot into the imaging system via the network?

- A. The computer's CMOS battery failed.
- B. The computer's NIC is faulty.
- C. The PXE boot option has not been enabled
- D. The Ethernet cable the technician is using to connect the desktop to the network is faulty.

Answer: C

Explanation:

The most likely reason the computer is unable to boot into the imaging system via the network is that the PXE boot option has not been enabled. PXE (Preboot Execution Environment) is an environment that allows computers to boot up over the network, instead of from a local disk. In order for this to work, the PXE boot option must be enabled in the computer's BIOS settings. As stated in the CompTIA A+ Core 2 exam objectives, technicians should know how to enable PXE in BIOS to enable network booting on a computer.

NEW QUESTION 5

Which of the following OS types provides a lightweight option for workstations that need an easy-to-use browser-based interface?

- A. FreeBSD
- B. Chrome OS
- C. macOS
- D. Windows

Answer: B

Explanation:

Chrome OS provides a lightweight option for workstations that need an easy-to-use browser-based interface

NEW QUESTION 6

A department has the following technical requirements for a new application:

```

Quad Core processor
250GB of hard drive space
6GB of RAM
Touch screens

```

The company plans to upgrade from a 32-bit Windows OS to a 64-bit OS. Which of the following will the company be able to fully take advantage of after the upgrade?

- A. CPU
- B. Hard drive
- C. RAM
- D. Touch screen

Answer: C

Explanation:

<https://www.makeuseof.com/tag/difference-32-bit-64-bit-windows/>

After upgrading from a 32-bit Windows OS to a 64-bit OS, the company will be able to fully take advantage of the RAM of the computer. This is because a 64-bit operating system is able to use larger amounts of RAM compared to a 32-bit operating system, which may benefit the system's overall performance if it has more than 4GB of RAM installed

NEW QUESTION 7

A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

- A. Scope of change
- B. Risk level
- C. Rollback plan
- D. End user acceptance

Answer: C

Explanation:

The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

NEW QUESTION 8

Each time a user tries to go to the selected web search provider, a different website opens. Which of the following should the technician check FIRST?

- A. System time
- B. IP address
- C. DNS servers
- D. Windows updates

Answer: C

Explanation:

When a user experiences unexpected or erratic behavior while browsing the internet, it could be caused by the DNS servers. DNS translates human-readable domain names (like google.com) into IP addresses, which computers can use to communicate with web servers. If the DNS servers are not functioning correctly or have been compromised, it can result in the browser being redirected to unintended websites.

NEW QUESTION 9

A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?

- A. The instructions from the software company are not being followed.
- B. Security controls will treat automated deployments as malware.
- C. The deployment script is performing unknown actions.
- D. Copying scripts off the internet is considered plagiarism.

Answer: C

Explanation:

The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data.

NEW QUESTION 10

A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

- A. Scan the computer with the company-provided antivirus software
- B. Install a new hard drive and clone the user's drive to it
- C. Deploy an ad-blocking extension to the browser.
- D. Uninstall the company-provided antivirus software
- E. Click the link in the messages to pay for virus removal
- F. Perform a reset on the user's web browser

Answer: CF

Explanation:

"The user thought the company-provided antivirus software would prevent this issue."

The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

NEW QUESTION 10

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

- A. A bad antivirus signature update was installed.
- B. A router was misconfigured and was blocking traffic.
- C. An upstream internet service provider was flapping.

D. The time or date was not in sync with the website.

Answer: B

Explanation:

The most likely cause of this issue is that a router was misconfigured and was blocking traffic. This would explain why remote users who were not connected to corporate resources did not have any issues.

NEW QUESTION 12

Which of the following command-line tools will delete a directory?

- A. md
- B. del
- C. dir
- D. rd
- E. cd

Answer: D

Explanation:

To delete an empty directory, enter `rd Directory` or `rmdir Directory`. If the directory is not empty, you can remove files and subdirectories from it using the `/s` switch. You can also use the `/q` switch to suppress confirmation messages (quiet mode).

NEW QUESTION 14

The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

- A. Data usage limits
- B. Wi-Fi connection speed
- C. Status of airplane mode
- D. System uptime

Answer: B

Explanation:

The technician should check the Wi-Fi connection speed first to troubleshoot this issue. Slow web browsing speed on a mobile phone can be caused by a slow Wi-Fi connection. The technician should check the Wi-Fi connection speed to ensure that it is fast enough to support web browsing. If the Wi-Fi connection speed is slow, the technician should troubleshoot the Wi-Fi network to identify and resolve the issue.

NEW QUESTION 15

A user's mobile phone has become sluggish. A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

- A. Prevent a device root
- B. Disable biometric authentication
- C. Require a PIN on the unlock screen
- D. Enable developer mode
- E. Block a third-party application installation
- F. Prevent GPS spoofing

Answer: CE

Explanation:

To help secure the device against this threat in the future, the administrator should require a PIN on the unlock screen and block a third-party application installation. Requiring a PIN on the unlock screen can help to prevent unauthorized access to the device, while blocking third-party application installation can help to prevent malicious applications from being installed on the device.

NEW QUESTION 19

An organization is centralizing support functions and requires the ability to support a remote user's desktop. Which of the following technologies will allow a technician to see the issue along with the user?

- A. RDP
- B. VNC
- C. SSH
- D. VPN

Answer: B

Explanation:

VNC will allow a technician to see the issue along with the user when an organization is centralizing support functions and requires the ability to support a remote user's desktop.

NEW QUESTION 20

A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?

- A. Registry Editor

- B. Task Manager
- C. Event Viewer
- D. Local Users and Groups

Answer: B

Explanation:

The technician would most likely use the Task Manager tool to safely make this change

The Task Manager tool can be used to disable applications from starting automatically on Windows 10

The tool that a technician would most likely use to stop an application from automatically starting when a user logs in to a Windows 10 system is the Task Manager. The Task Manager can be used to view and manage processes, including those that are set to automatically start when a user logs in to the system.

NEW QUESTION 23

A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?

- A. Turn off airplane mode while at the register.
- B. Verify that NFC is enabled.
- C. Connect to the store's Wi-Fi network.
- D. Enable Bluetooth on the phone.

Answer: B

Explanation:

The user should verify that NFC is enabled on their phone. NFC is a technology that allows two devices to communicate with each other when they are in close proximity.

NFC (Near Field Communication) technology allows a phone to wirelessly communicate with a payment terminal or other compatible device. In order to use NFC to make a payment or transfer information, the feature must be enabled on the phone. Therefore, the user should verify that NFC is enabled on their phone before attempting to make a payment with it. The other options, such as turning off airplane mode, connecting to Wi-Fi, or enabling Bluetooth, do not pertain to the NFC feature and are unlikely to resolve the issue. This information is covered in the CompTIA A+ Core2 documents/guide under the Mobile Devices section.

NEW QUESTION 25

An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

- A. Risk analysis
- B. Sandbox testing
- C. End user acceptance
- D. Lessons learned

Answer: A

Explanation:

A risk analysis must be completed before a change request for an upcoming server deployment can be approved

Risk analysis is an important step in the change management process because it helps identify and mitigate potential risks before changes are implemented. Once the risks have been analyzed and the appropriate measures have been taken to minimize them, the change can be approved and implemented.

NEW QUESTION 28

A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

- A. Remote wipe
- B. Anti-malware
- C. Device encryption
- D. Failed login restrictions

Answer: A

Explanation:

The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device.

NEW QUESTION 30

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

- A. Security and Maintenance
- B. Network and Sharing Center
- C. Windows Defender Firewall
- D. Internet Options

Answer: D

Explanation:

The best choice for accessing the necessary configuration to configure the desktop systems to use a new proxy server is the Internet Options utility. This utility can be found in the Control Panel and allows you to configure the proxy settings for your network connection. As stated in the CompTIA A+ Core 2 exam objectives, technicians should be familiar with the Internet Options utility and how to configure proxy settings.

NEW QUESTION 34

A new spam gateway was recently deployed at a small business. However, users still occasionally receive spam. The management team is concerned that users will open the messages and potentially infect the network systems. Which of the following is the MOST effective method for dealing with this issue?

- A. Adjusting the spam gateway
- B. Updating firmware for the spam appliance
- C. Adjusting AV settings
- D. Providing user training

Answer: D

Explanation:

The most effective method for dealing with spam messages in a small business is to provide user training. Users should be trained to recognize spam messages and avoid opening them. They should also be trained to report spam messages to the IT department so that appropriate action can be taken. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems.

NEW QUESTION 37

A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

- A. Right-click the Windows button, then select Run, entering shell startup and clicking OK, and then move items one by one to the Recycle Bin
- B. Remark out entries listed HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run
- C. Manually disable all startup tasks currently listed as enabled and reboot, checking for issue resolution at startup
- D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.

Answer: D

Explanation:

This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

NEW QUESTION 38

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

- A. ipconfig /all
- B. hostname
- C. netstat /?
- D. nslookup localhost
- E. arp -a
- F. ping :: 1

Answer: AB

Explanation:

The user can use the following commands to give the technician the correct information: ipconfig /all and hostname. The ipconfig /all command displays the IP address, subnet mask, and default gateway for all adapters on the computer. The hostname command displays the name of the computer.

NEW QUESTION 43

A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

- A. resmon.exe
- B. dfrgui.exe
- C. msinfo32.exe
- D. msconfig.exe

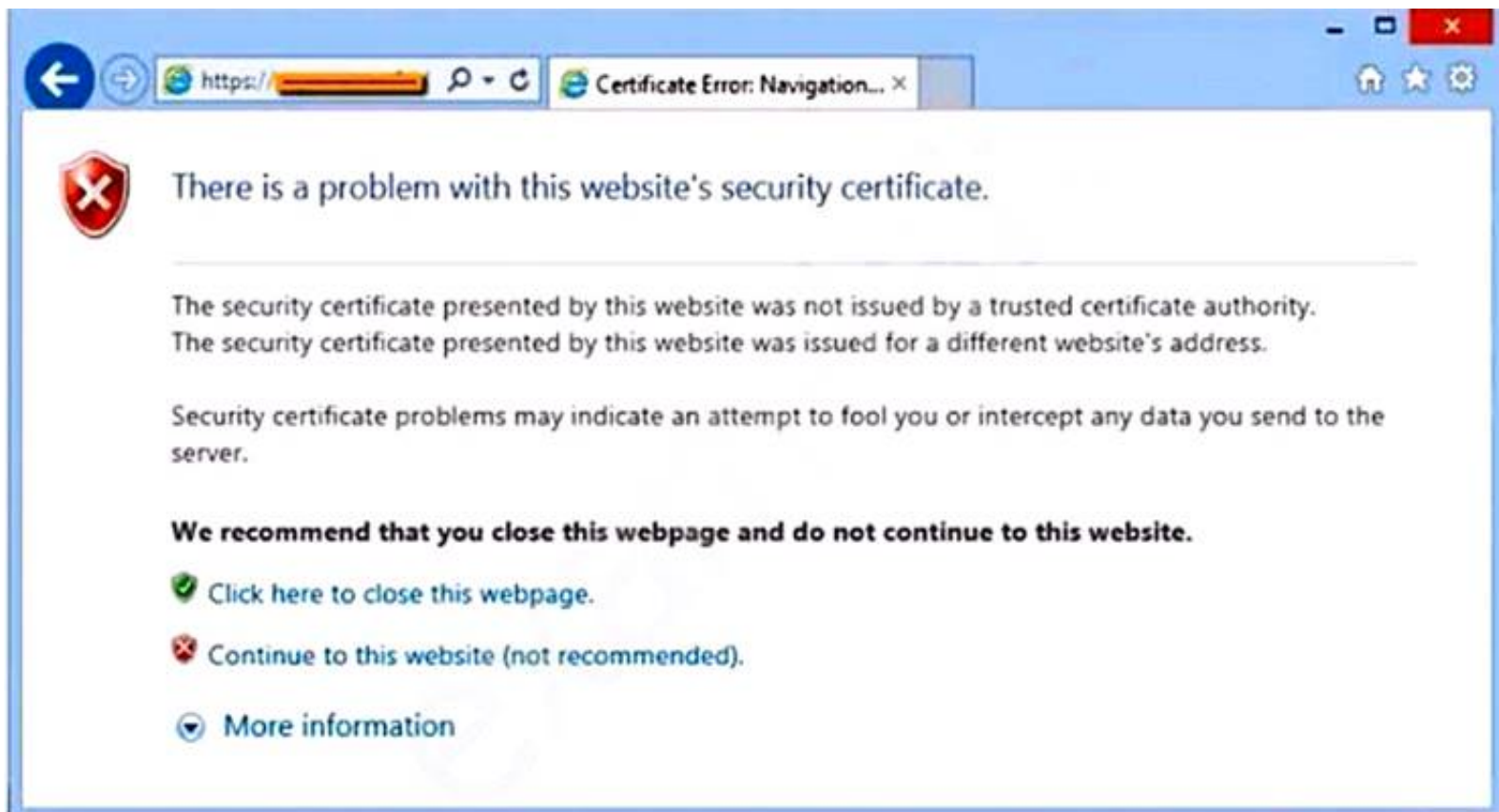
Answer: A

Explanation:

If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O. Resource Monitor provides detailed information about the system's resource usage, including disk I/O. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action.

NEW QUESTION 46

After clicking on a link in an email, a Chief Financial Officer (CFO) received the following error:



The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

- A. Update the browser's CRLs
- B. File a trouble ticket with the bank.
- C. Contact the ISP to report the CFCs concern
- D. Instruct the CFO to exit the browser

Answer: A

Explanation:

The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

NEW QUESTION 49

A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

- A. Drilling
- B. Degaussing
- C. Low-level formatting
- D. Erasing/wiping

Answer: D

Explanation:

Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

NEW QUESTION 52

Which of the following is a data security standard for protecting credit cards?

- A. PHI
- B. NIST
- C. PCI
- D. GDPR

Answer: C

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

NEW QUESTION 53

Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?

- A. Network and Sharing Center
- B. Programs and Features
- C. Default Apps
- D. Add or Remove Programs

Answer: C

Explanation:

Default Apps should be used to ensure all PDF files open in Adobe Reader1

NEW QUESTION 56

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A. FAT32
- B. ext4
- C. NTFS
- D. exFAT

Answer: D

Explanation:

exFAT is a file system that is supported by both Linux and Windows and can handle large files¹.

NEW QUESTION 58

A desktop support technician is tasked with migrating several PCs from Windows 7 Pro to Windows 10 Pro. The technician must ensure files and user preferences are retained, must perform the operation locally, and should migrate one station at a time. Which of the following methods would be MOST efficient?

- A. Golden image
- B. Remote network install
- C. In-place upgrade
- D. Clean install

Answer: C

Explanation:

An in-place upgrade is the most efficient method for migrating from Windows 7 Pro to Windows 10 Pro, as it will retain all user files and preferences, can be done locally, and can be done one station at a time. An in-place upgrade involves installing the new version of Windows over the existing version, and can be done quickly and easily.

NEW QUESTION 61

A technician is tasked with configuring a computer for a visually impaired user. Which of the following utilities should the technician use?

- A. Device Manager
- B. System
- C. Ease of Access Center
- D. Programs and Features

Answer: C

Explanation:

The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

NEW QUESTION 62

Which of the following is the MOST important environmental concern inside a data center?

- A. Battery disposal
- B. Electrostatic discharge mats
- C. Toner disposal
- D. Humidity levels

Answer: D

Explanation:

One of the most important environmental concerns inside a data center is the level of humidity. High levels of humidity can cause condensation, which can result in corrosion of components and other equipment. Low levels of humidity can cause static electricity to build up, potentially leading to electrostatic discharge (ESD) and damage to components. Therefore, it is crucial to maintain a relative humidity range of 40-60% in a data center to protect the equipment and ensure proper operation.

NEW QUESTION 63

A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

- A. The GPS application is installing software updates.
- B. The GPS application contains malware.
- C. The GPS application is updating its geospatial map data.
- D. The GPS application is conflicting with the built-in GPS.

Answer: B

Explanation:

The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phone.

NEW QUESTION 67

A suite of security applications was installed a few days ago on a user's home computer. The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

- A. Services in Control Panel to check for overutilization
- B. Performance Monitor to check for resource utilization
- C. System File Checker to check for modified Windows files
- D. Event Viewer to identify errors

Answer: C

Explanation:

System File Checker to check for modified Windows files. System File Checker (SFC) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applications [1][2]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.

NEW QUESTION 71

A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

- A. Installer_x64.exe
- B. Installer_Files.zip
- C. Installer_32.msi
- D. Installer_x86.exe
- E. Installer_Win10Enterprise.dmg

Answer: D

Explanation:

The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture.

<https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/>

NEW QUESTION 76

A field technician applied a Group Policy setting to all the workstations in the network. This setting forced the workstations to use a specific SNTP server. Users are unable to log in now. Which of the following is the MOST likely cause of this issue?

- A. The SNTP server is offline.
- B. A user changed the time zone on a local machine.
- C. The Group Policy setting has disrupted domain authentication on the system,
- D. The workstations and the authentication server have a system clock difference.

Answer: D

Explanation:

The workstations and the authentication server have a system clock difference. If a Group Policy setting is applied that forces the workstations to use a specific SNTP server, but the system clock on the workstations and the authentication server are out of sync, then this can cause authentication issues and users will be unable to log in. In this case, the most likely cause of the issue is a difference in system clocks and the technician should ensure that the clocks on the workstations and the authentication server are in sync.

NEW QUESTION 78

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A. FAT32
- B. ext4
- C. NTFS
- D. exFAT

Answer: C

Explanation:

Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

NEW QUESTION 79

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

- A. File Explorer
- B. User Account Control
- C. Windows Backup and Restore
- D. Windows Firewall
- E. Windows Defender
- F. Network Packet Analyzer

Answer: AE

Explanation:

The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software¹

NEW QUESTION 81

A Microsoft Windows PC needs to be set up for a user at a large corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

- A. Windows Enterprise Edition
- B. Windows Professional Edition
- C. Windows Server Standard Edition
- D. Windows Home Edition

Answer: B

Explanation:

The Windows Professional Edition is the most likely version that a technician would deploy for a user at a target corporation. This version of Windows is designed for business use and provides the necessary features and capabilities that a user would need to access the corporate domain, such as email and shared drives.

NEW QUESTION 86

A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

- A. Disk Cleanup
- B. Group Policy Editor
- C. Disk Management
- D. Resource Monitor

Answer: D

Explanation:

Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

NEW QUESTION 88

A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible. Which of the following backup methods should the technician MOST likely implement?

- A. Full
- B. Mirror
- C. Incremental
- D. Differential

Answer: C

Explanation:

The law firm wants to retain more versions of the backups when possible, so the best backup method for the technician to implement in this scenario would be Incremental backup. Incremental backups only save the changes made since the last backup, which allows for more frequent backups and minimizes the amount of storage required. This would allow the law firm to retain more than three versions of backups without risking backup failure.

To retain more versions of backups, the technician should implement an Incremental backup method¹

An incremental backup method only backs up the data that has changed since the last backup, so it requires less storage space than a full backup²

NEW QUESTION 93

A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?

- A. Ransomware
- B. Failed OS updates
- C. Adware
- D. Missing system files

Answer: B

Explanation:

The most likely reason for the antivirus protection on a company laptop being out of date is failed OS updates¹. Antivirus software relies on the operating system to function properly. If the operating system is not up-to-date, the antivirus software may not function properly and may not be able to receive the latest virus definitions and updates². Therefore, it is important to keep the operating system up-to-date to ensure the antivirus software is functioning properly².

NEW QUESTION 95

A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

- A. Deploy a secondary hard drive with encryption on the appropriate workstation
- B. Configure a hardened SFTP portal for file transfers between file servers

- C. Require files to be individually password protected with unique passwords
- D. Enable BitLocker To Go with a password that meets corporate requirements

Answer: D

Explanation:

The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

NEW QUESTION 97

A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

- A. Keyboard
- B. Touch pad
- C. Ease of Access Center
- D. Display settings

Answer: C

Explanation:

The OS utility used to change the color of the cursor in Windows is Ease of Access Center.

The user can change the cursor color by opening the Settings app, selecting Accessibility in the left sidebar selecting Mouse pointer and touch under Vision, and choosing one of the cursor options. The user can select Custom to pick a color and use the Size slider to make the cursor larger or smaller.

The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the CompTIA A+ Core2 documents/guide under the Accessibility section.

NEW QUESTION 98

A small business owner wants to install newly purchased software on all networked PCs. The network is not configured as a domain, and the owner wants to use the easiest method possible. Which of the following is the MOST deficient way for the owner to install the application?

- A. Use a network share to share the installation files.
- B. Save software to an external hard drive to install.
- C. Create an imaging USB for each PC.
- D. Install the software from the vendor's website

Answer: B

Explanation:

Saving software to an external hard drive and installing it on each individual PC is the most inefficient method for the small business owner. This method requires manual intervention on each PC, and there is a higher risk of error or inconsistencies between PCs. Additionally, if the software needs to be updated or reinstalled in the future, this process would need to be repeated on each PC.

NEW QUESTION 103

A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

- A. Application updates
- B. Anti-malware software
- C. OS reinstallation
- D. File restore

Answer: C

Explanation:

If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system.
<https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html>

NEW QUESTION 105

A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician is unable to find this menu item?

- A. The hardware does not meet BitLocker's minimum system requirements.
- B. BitLocker was renamed for Windows 10.
- C. BitLocker is not included on Windows 10 Home.
- D. BitLocker was disabled in the registry of the laptop

Answer: C

Explanation:

BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions. Therefore, the technician is unable to find the BitLocker Drive Encryption menu item in Control Panel because it is not included in the Windows 10 Home edition.

NEW QUESTION 106

A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

- A. Configure the network as private
- B. Enable a proxy server
- C. Grant the network administrator role to the user
- D. Create a shortcut to public documents

Answer: A

Explanation:

The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

NEW QUESTION 111

A user created a file on a shared drive and wants to prevent its data from being accidentally deleted by others. Which of the following applications should the technician use to assist the user with hiding the file?

- A. Device Manager
- B. Indexing Options
- C. File Explorer
- D. Administrative Tools

Answer: C

Explanation:

The technician should use the File Explorer application to assist the user with hiding the file 1. The user can right-click the file and select Properties. In the Properties dialog box, select the Hidden check box, and then click OK 1.

NEW QUESTION 113

Which of the following change management documents includes how to uninstall a patch?

- A. Purpose of change
- B. Rollback plan
- C. Scope of change
- D. Risk analysis

Answer: B

Explanation:

The change management document that includes how to uninstall a patch is called the “rollback plan”. The rollback plan is a document that outlines the steps that should be taken to undo a change that has been made to a system. In the case of a patch, the rollback plan would include instructions on how to uninstall the patch if it causes problems or conflicts with other software12

NEW QUESTION 117

A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

- A. Run the virus scanner in an administrative mode.
- B. Reinstall the operating system.
- C. Reboot the system in safe mode and rescan.
- D. Manually delete the infected files.

Answer: C

Explanation:

Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

NEW QUESTION 118

A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

- A. Enable multifactor authentication.
- B. Increase the failed log-in threshold.
- C. Remove complex password requirements.
- D. Implement a single sign-on with biometrics.

Answer: A

Explanation:

Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

NEW QUESTION 120

A developer is creating a shell script to automate basic tasks in Linux. Which of the following file types are supported by default?

- A. .py
- B. .js
- C. .vbs
- D. .sh

Answer: D

Explanation:

<https://www.educba.com/shell-scripting-in-linux/>

NEW QUESTION 123

Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

- A. Pretexting
- B. Spoofing
- C. Vishing
- D. Scareware

Answer: C

Explanation:

Vishing is a type of social engineering attack where a fraudulent caller impersonates a legitimate entity, such as a bank or financial institution, in order to gain access to sensitive information. The caller will typically use a variety of techniques, such as trying to scare the target or providing false information, in order to get the target to provide the information they are after. Vishing is often used to gain access to usernames, passwords, bank account information, and other sensitive data.

NEW QUESTION 127

A technician needs to exclude an application folder from being cataloged by a Windows 10 search. Which of the following utilities should be used?

- A. Privacy
- B. Indexing Options
- C. System
- D. Device Manager

Answer: B

Explanation:

To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options utility

NEW QUESTION 130

Which of the following is MOST likely contained in an EULA?

- A. Chain of custody
- B. Backup of software code
- C. Personally identifiable information
- D. Restrictions of use

Answer: D

Explanation:

An EULA (End-User License Agreement) is a legally binding contract between a software supplier and a customer or end-user, generally made available to the customer via a retailer acting as an intermediary. A EULA specifies in detail the rights and restrictions which apply to the use of the software. Some of the main terms included in an EULA are the terms and scope of the license, any licensing fees, warranties and disclaimers, limitation of liability, revocation or termination of the license, and intellectual property information and restrictions on using the license (e.g. modification and copying)

<https://www.termsfeed.com/blog/eula-vs-terms-conditions/>

NEW QUESTION 133

A technician is investigating an employee's smartphone that has the following symptoms

- The device is hot even when it is not in use.
- Applications crash, especially when others are launched
- Certain applications, such as GPS, are in portrait mode when they should be in landscape mode

Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

- A. Turn on autorotation
- B. Activate airplane mode.
- C. Close unnecessary applications
- D. Perform a factory reset
- E. Update the device's operating system
- F. Reinstall the applications that have crashed.

Answer: AC

Explanation:

The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature

NEW QUESTION 138

A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

- A. .deb
- B. .vbs
- C. .exe
- D. .app

Answer: D

Explanation:

The file type that the technician will MOST likely use when installing new software on a macOS computer is .app. This is because .app is the file extension for applications on macOS.

NEW QUESTION 140

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

220-1102 Practice Exam Features:

- * 220-1102 Questions and Answers Updated Frequently
- * 220-1102 Practice Questions Verified by Expert Senior Certified Staff
- * 220-1102 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 220-1102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 220-1102 Practice Test Here](#)